Wireshark Project: Network Traffic Analysis and Security Threat Identification

Objective:

The goal of this project is to capture and analyze network traffic using Wireshark to identify potential security threats, such as malware, unauthorized access, and data exfiltration. I will follow steps to capture live traffic, filter traffic for specific protocols, and analyze suspicious activity within the captured data.

Project Outline:

1. Network Environment Setup

For this project, I will set up a network environment to capture and analyze traffic. The network will include multiple devices (e.g., a server, client machines, and possibly a simulated attacker) communicating over various protocols.

Tools Required:

- Wireshark: Network traffic analyzer.
- Network Devices: One or more computers (physical or virtual) to simulate real-world network activity.
- Virtual Machines: (Optional) Using VirtualBox or VMware to simulate network traffic across different environments.
- Attack Simulation Tools: (Optional) Tools like Metasploit or Kali Linux to simulate network attacks (e.g., DoS attacks, SQL injections, etc.).

2. Capturing Network Traffic

Steps:

- I will configure Wireshark to capture all incoming and outgoing network traffic on my machine.
- I will select the appropriate network interface to monitor traffic (e.g., Wi-Fi or Ethernet).
- Then, I will start capturing and let Wireshark run for 10-15 minutes while performing routine network tasks (e.g., browsing, downloading files, accessing services).

Objective:

My goal is to capture and save network traffic that includes both standard user activities (HTTP, HTTPS, DNS queries) and any potential anomalies (e.g., an attacker's scanning or phishing attempts).

3. Protocol Filtering and Traffic Analysis

To analyze specific types of traffic, I will apply Wireshark filters to focus on certain protocols. For this project, I will focus on:

- HTTP and HTTPS: To examine web traffic, identify requests and responses between clients and servers.
- DNS: I will filter DNS traffic to identify potential attempts to resolve malicious domain names.
- TCP/UDP: I will focus on unusual or high-volume traffic that might indicate port scans or flooding attempts.
- FTP/SSH: I will detect potential unauthorized file transfers or remote logins.

Steps:

- I will use filters like http, dns, tcp.port==80 or tcp.port==443, and ip.addr==[Target IP Address].
- I will analyze packet details to uncover anomalies, such as suspicious IP addresses, abnormal

traffic patterns, or repeated failed connection attempts.

Objective:

I will apply filtering techniques to zoom in on relevant data streams and eliminate unnecessary noise. I will identify potential anomalies by carefully reviewing traffic for inconsistencies or irregularities.

4. Identifying Security Threats

Types of Threats to Look For:

- Malware Communications: I will look for abnormal outbound connections to suspicious IP addresses or domains.
- Phishing Attempts: I will examine email traffic to identify instances where employees may have received phishing emails containing malicious attachments or links.
- Data Exfiltration: I will identify large outbound traffic sessions to unfamiliar external IPs, which might indicate that sensitive data is being leaked.
- Unauthorized Access: I will look for suspicious login attempts or remote access through protocols like SSH, indicating a possible breach.

Analysis Methodology:

- Inspect Suspicious IPs: I will use external resources like VirusTotal to check whether the IP addresses or domains found in the traffic have been flagged as malicious.
- Inspect HTTP/HTTPS Requests: I will examine user-agent strings, cookie headers, and payloads for signs of tampering or injection attacks (e.g., SQL injection).
- Analyze DNS Queries: I will look for abnormal domain requests that could indicate command-and-control (C2) servers for malware.

Objective:

Using Wireshark, I will identify and document at least three potential security threats from the captured network traffic. I will provide a detailed explanation of each, supported by evidence (e.g., packet captures, unusual payloads).

5. Reporting and Documentation

Key Areas to Document:

1. Network Capture Summary:

- Total packets captured, duration of capture, and any significant traffic statistics.

2. Suspicious Traffic:

- I will detail any suspicious IP addresses, domains, or URLs identified during analysis.

3. Threats Identified:

- For each threat identified (e.g., malware, unauthorized access), I will document:
  - The type of threat.
  - The traffic and protocols involved.
  - Screenshots of Wireshark packet captures showing the suspicious activity.
  - Potential consequences if the threat went unmitigated.

4. Remediation Recommendations:

- For each threat, I will provide recommendations for mitigation (e.g., implementing firewalls, enabling Intrusion Detection Systems, regular traffic analysis).

Objective:

I will prepare a professional report summarizing my findings, complete with screenshots of key traffic captures, analysis of potential threats, and recommendations for preventing future attacks.

6. Security Controls and Prevention

Security Controls to Implement:

1. Intrusion Detection System (IDS): I will implement an IDS to monitor for unusual traffic patterns and automatically flag suspicious activity.

2. Firewall Rules: I will refine firewall rules to block traffic from suspicious IP ranges or restrict access to certain services from external networks.

3. Regular Vulnerability Scanning: I will schedule vulnerability scans to proactively identify weaknesses in the network infrastructure.

4. Employee Training: I will ensure employees are trained on phishing awareness to reduce the chances of falling for malicious email-based attacks.

Objective:

I will implement a list of actionable security controls based on my findings, explaining how they will help secure the network environment against future attacks.

7. Conclusion

In conclusion, this project highlights how Wireshark can be a critical tool for security analysts to monitor network traffic, identify threats, and respond to incidents. Continuous network traffic analysis is crucial in maintaining a secure and resilient IT infrastructure.